A Comparison of Critical Infrastructure Resilience Quantification Techniques

M. Imani[a], D. Hajializadeh[a]

[a] Department of Engineering and the Built Environment (EBE),
Anglia Ruskin University

Abstract: Promoting the resilience of critical infrastructure, when subjected to different hazardous events, is vital. However, applying inappropriate and/or imprecise resilience metrics or quantification techniques could increase the costs of resilience enhancement and reduce its effectiveness in critical infrastructure. This paper develops a method to evaluate and compare different resilience quantification techniques, in relation to different system failure states, in order to measure their effectiveness.

1 Introduction

Disastrous events such as extreme weather events are increasing every day and causing extensive damage to the critical transportation, water and energy infrastructure. Consequently, adopting adaptive measures to increase resilience is becoming more important as the severity of extreme weather events, and their effect on society, security and the economy, increases. Therefore, there is a global consensus that the critical infrastructure resilience needs promotion. A resilient system reacts quickly in which the consequence of occurrence of any inconvenience/impact on the system is minimised. On the contrary, a vulnerable system can result to a high level of distress, as it is not able to respond to the strains. In synthesis, a vulnerable system discharges a more negative and heavier impact on its users and manager whereas a resilient system functions in such a way that the users and managers do not experience any negative impact on usual infrastructure functionality and service.

To assess the level of resilience of any infrastructure system it is important to define resilience and its metrics first. Resilience is a concept intertwined with vulnerability, intended as series of elements present within a system, prior to the occurrence of hazards, which can affect ability of the system to cope with and recover from the resulting impacts. Collectively literature contains a wide range of definitions, metrics and measurement methodologies proposed for critical infrastructure resilience quantification. For example, resilience has been defined as the ability of a system, community, society to "resist the impact of a natural or social event" [8], "to react and recover from the damaging effect of realized hazards" [4]; and "the capacity for renewal, reorganization and development" [5]. [1] defines the resilience as the difference from full performance to disrupted performance (from time where disruption occurs to time which system returns to its normal pre-disruption. [9] uses the same Triangle resilience idea and defines the loss of resilience as the percentage of the total possible loss over some suitably long time interval. [6] defines resilience as ratio of recovery to loss. However, a standardised metric or measurement for resilience, which assures its effectiveness and keeping the promotion cost at an acceptable level, remains a challenging to [7]. This study addresses this issue by evaluating the

correlation between the system behaviour and a few selected widely used resilience metrics. This study is limited to metric and formula for infrastructure resilience. [2] suggest that resilience has four dimensions: 1. Technical dimension: focusing on system's performance after a shock hits; 2.organizational: focusing on the organisations' ability to respond to the challenge posed by the hazard and still carry out their key functions; 3.social: "the capacity to reduce the negative societal consequences of loss of critical services" and 4. economic: referring to the ability of avoiding economic losses as a consequence of the disaster.
This study only focuses on the technical dimension in which the functionality has been used to quantify system resilience (so-called operational resilience). There are a series of metrics that can be used to quantify system resilience. In this article, five widely used metrics have been reviewed and applied to a simple hypothetical benchmark network to illustrate differences in the quantification techniques. These techniques and their application to case study are provided in section 2.4.

2 Method of Analysis

In this study, global resilience approach is adopted to evaluate the performance of a simple benchmark network when subject to a range of failure states (FS). Figure 1 demonstrates the flowchart of the methodology for global resilience evaluation in this study. The methodology comprises of three following sections:

- Network failure state: this section characterises the failure type(s) and failed element(s) (what fail/failed);
- Network operational fluctuation: this section illustrates network elements' (e.g. nodes, links) potential behavioural change in response to the FS(s);
- Resilience evaluation: this section adopts six widely used resilience quantification methods to evaluate the benchmark network resiliency by incorporating the FS(s) and operational fluctuation(s) into the evaluation process.

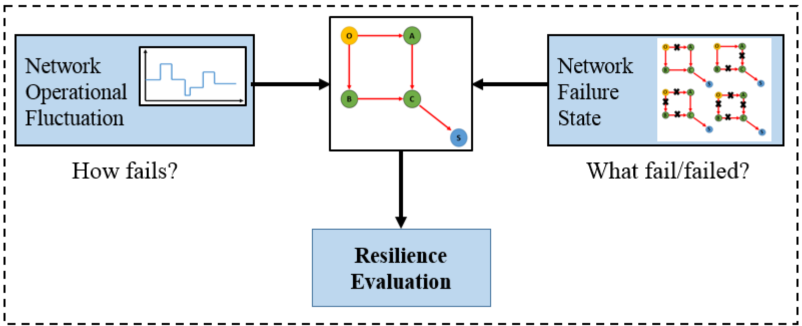

Figure 1: Flowchart of the methodology

2.1 Benchmark Network

For this study, a simple hypothetical benchmark network, with five nodes (including source and sink nodes) and five links (see Figure 2), was created for global resilience evaluation. This benchmark network is a very simple and miniaturised version of similar infrastructure networks (e.g. water supply system, railway and road system and so on) therefore the technique can be expanded, adapted and applied to complicated networks.

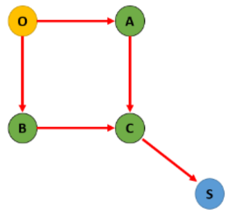

Figure 2: Hypothetical benchmark network

2.2 Network Failure State

Failure State represents the existing condition (operational condition and/or physical condition) of a network that has the potential to cause network failure (partially or fully), regardless of the origin, type and severity of the initial hazardous event (e.g. extreme rainfall, earthquake, etc.). To characterise a network FS, type (operational/physical; partially/fully) and location (node/link) of that should be determined (what fail/failed).
In this benchmark network, two FSs could be characterised: node failure and link failure. Nevertheless, in a real network, FSs will have operational and/or physical context. For example, in water distribution systems: pressure drop, pump failure, pipe leakage; in sewer system: pipe blockage; in transport system: road closure, accident. In this study, global resilience is evaluated when the network is subject to link(s) failure involving random cumulative elements. Figure 4 presents sixteen potential FSs (i.e. link failure) for this benchmark network as, one link at a time – four scenarios; two links at a time – seven scenarios; three links at a time – four scenarios; four links at a time – one scenario.
Note: the link to the sink node is not included in the evaluation process for simplicity. In addition, in this study simultaneous FSs are assumed in this network (no particular order).

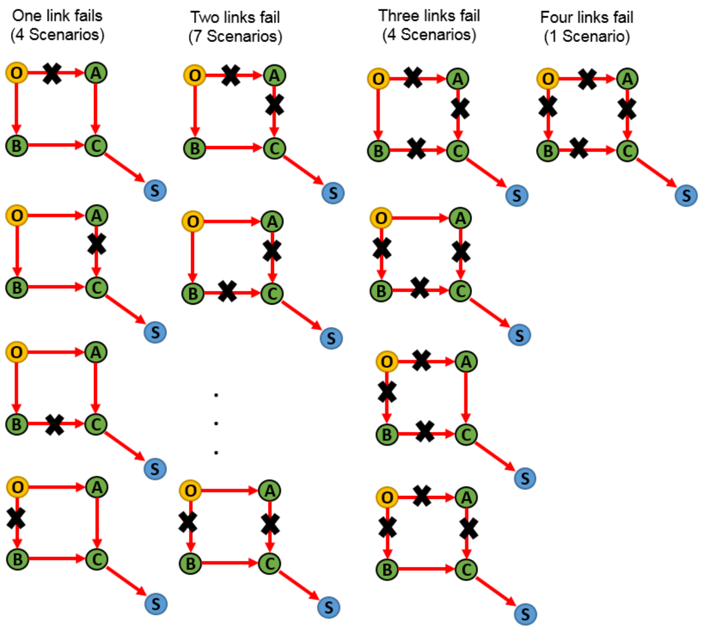

Figure 4: Network failure states

2.3 Network Operational Fluctuation

Interrupting events (shocks and stresses), regardless of their origin, type, duration, frequency and severity, will change the whole system behavior. These behavioral changes are arisen from aggregation of the operational fluctuations of the network elements. This study illustrates the aforementioned fluctuations as operational time series of each element. For example, in water supply system, this could be interpreted as the pipes pressure variation or in sewer system as manholes' surcharge and in transport system as traffic congestion in a road.

To study the operational fluctuations of each element, three parameters of duration of failure (F_{dur}), magnitude of failure (F_{mag}) and frequency of failure (F_{freq}) are taken into account (see Table 1). Each parameter will have two modes and their associated values. For simplicity, the values presented in Table 1, are dimensionless and scaled into the range [0-1].

Table 1: Network operational fluctuation modes

Parameter	**Mode**	**Value (dimensionless)**
Duration of failure (F_{dur})	Short	0.1
	Long	0.4
Magnitude of Failure (F_{mag})	Small	0.4
	Large	1
Frequency of failure (F_{freq})	Single Occurrence	1
	Frequent Occurrence	5

The above six modes constitute eight different operational fluctuation scenarios as outlined in Table 2.

Table 2: Network operational fluctuation scenarios

Short-Small-Single (SSS)	Long-Small-Single (LSS)
Short-Small-Frequent (SSF)	Long-Small-Frequent (LSF)
Short-Large-Single (SLS)	Long-Large-Single (LLS)
Short-Large-Frequent (SLF)	Long-Large-Frequent (LLF)

It should be noted that for simplicity in this study, frequent fluctuations (i.e. SSF, SLF, LSF, LLF in Table 2) will all have the same F_{dur} and F_{mag}. For instance, Figure 3 represents a LLF operational fluctuation scenario (OFS).

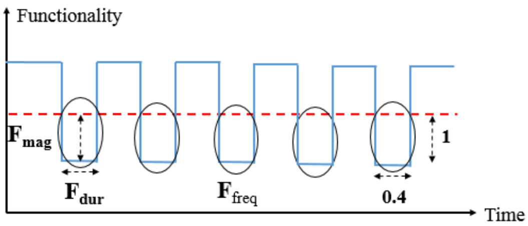

Figure 3: LLF network operational scenario

2.4 Resilience

In this study, six widely used resilience quantification methods, which are in fact surrogate measures of resilience, are used to evaluate the benchmark network performance. These methods are as follows:

- Bounce backability – Time Independent (BBA-TID): maximum flow to initial maximum flow [6];
- Residence time in Failure State (RFS): total duration of being in failure state [3];
- Residence time in non-Failure State (RNFS): total duration of not being in failure state [3];
- Time in Failure State (TFS): average time of being in failure state [3];
- Time in non-Failure State (TNFS): average time of not being in failure state [3].

2.5 Results

The current section presents the results of the analysis conducted on the case study illustrating differences between resilience metrics and OFS. Figure 4 illustrates the variation of different resilience metrics for different OFS in 100 realisation of Monte Carlo simulations in which the time lag is randomly generated. The horizontal axis in these figures corresponds to resilience metrics (five metrics) × OFS (six scenarios) and the vertical axis shows resilience value. Figure 1.a demonstrates that BBA-TID has minimum variation in all OFS, RFS, RNFS are next, which shows the independency of the resilience metrics with the time lag of failure. TNFS however illustrates the maximum variation in resilience metrics in which the metric is varying from zero to 0.8. Nevertheless, this variation has declined significantly when the number of failed links increase (i.e. Figures 4b-d). The opposite phenomenon is happening for the BBA-TID, RFS and RNFS metrics, which are quite consistent in one link failure scenario. This can be explained by the fact that bounce backability metric can significantly vary when the time lags of failed links synchronized and result in bigger variation. Given that the network sample chosen for this study only contains five links, variation in time lag cannot make huge difference in failure or non-failure state duration. This explains the small variation of these metrics in scenarios with more than one failed link.

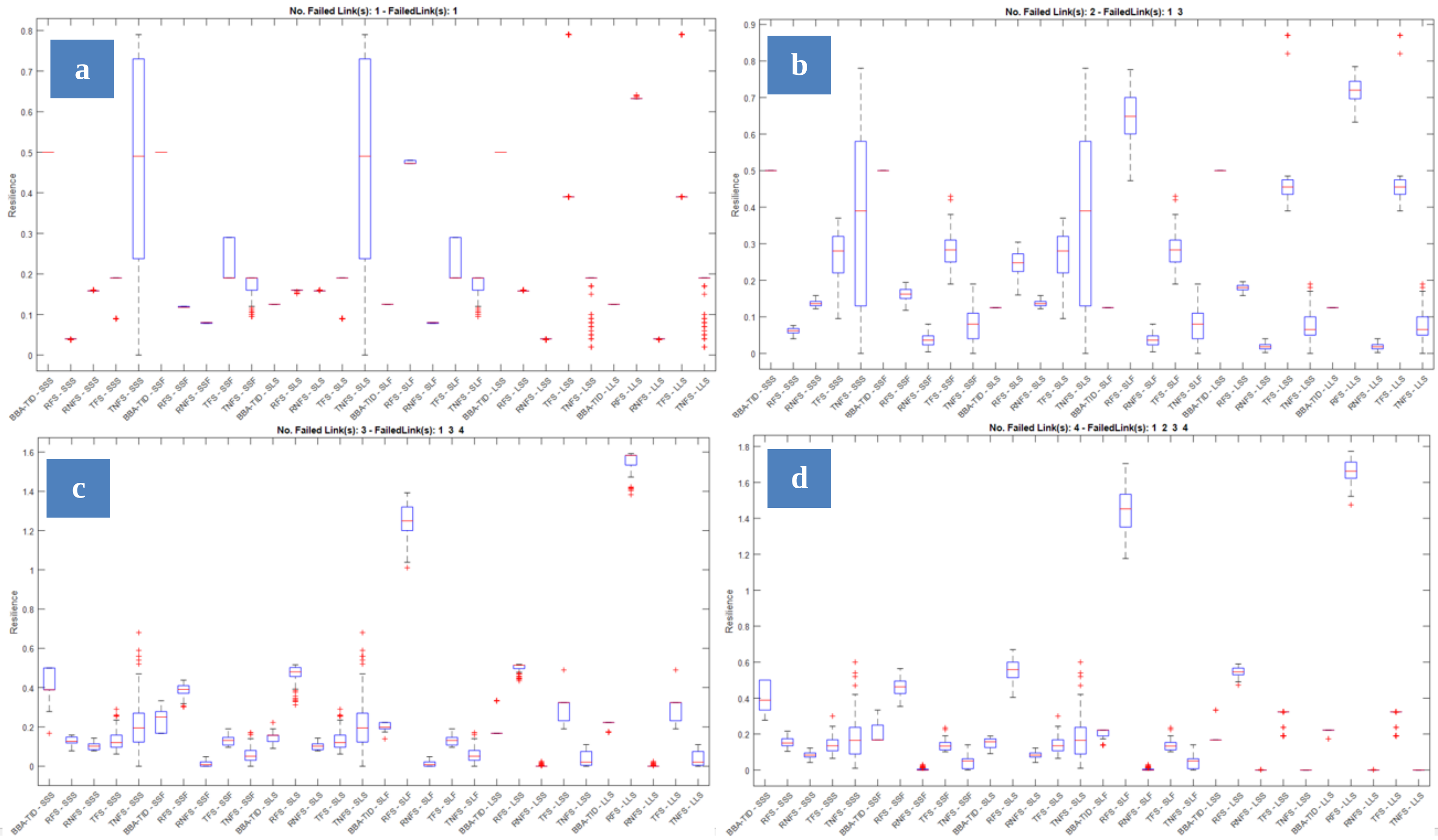

Figure 4: resilience variation in all potential failure states of the network;
***a:** no. of failed links: 1, link no.: 1; **b:** no. of failed links: 2, link no.: 1, 3;*
***c:** no. of failed links: 3, link no.: 1, 3, 4; **d:** no. of failed links: 4, link no.: 1,2,3,4*

Figure 5 illustrates the variation of resilience metrics for four selected links' OFS in area plot. Comparing different scenarios, it can be seen that TNFS is zero for link failure scenarios of 3-link and 4-link scenarios at SSF, SLF, LSS and LLS. Frequent failure state, long failure duration and high failure magnitude for failure scenarios with more than two links results in highest time in failure state (maximum RFS and TFS) which naturally would mean minimum TNFS (which also means minimum RNFS). This is also true for scenarios with two links on the opposite sides (i.e., 1 and 2/4 or 2 and 1/3) which result in zero flow in the network.

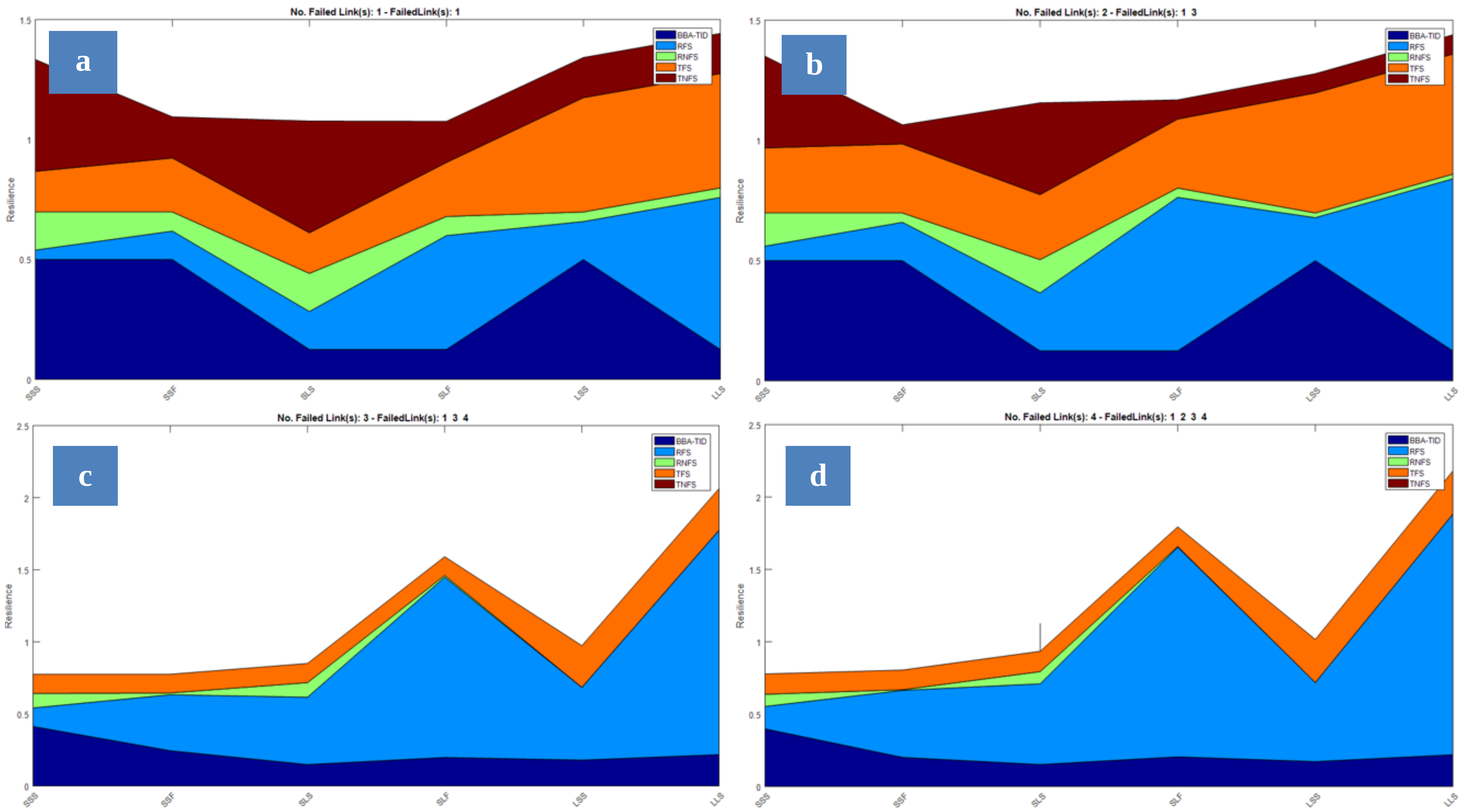

Figure 5: resilience variation in operatioanl fluctuations;
***a:** no. of failed links: 1, link no.: 1; **b:** no. of failed links: 2, link no.: 1, 3;*
***c:** no. of failed links: 3, link no.: 1, 3, 4; **d:** no. of failed links: 4, link no.: 1, 2, 3, 4*

In conclusion, by categorising the resilience metrics, it can be seen that RNFS, TNFS, BBA-TIS would fall in one category in which the resilience metric decreases by an increase in number of failed links. In these metrics, the failure of two links falls in two different subcategories in which failure of links from opposite sides results in higher value in comparison to failed links on one side (i.e., failure of link 1 and 2 result in higher value in comparison to failure of link 1 and 3). The RFS falls in the next category in which an increase in number of failed links increases the resilience metric. The TFS was expected to follow the same pattern; however, the result from 100 realisation of Monte Carlo simulation shows that this metric does not exactly fall in this pattern. In this metric, the 2-link failure scenarios in LLS and LSS result in lower value in comparison to 3-link and 4-link scenarios. This is not consistent with the pattern in other scenarios (i.e., SSS, SSF, SLS, and SLF) which is mainly due to the small difference between the resilience metric of 2-link, 3-link and 4-link scenarios.

References

[1] Bruneau, M. et al. *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities.* Earthquake Spectra, Vol. 19 (4): 733–752, 2003.

[2] Chang, S. E and Shinozuka, M. *Measuring Improvements in the disaster resilience of communities*, *Erathquake Spectra*, n.d.

[3] Fiering, M. B. *Alternative Indices of Resilience*. Water Resources Research, Vol. 18 (1), 33-39, 1982.

[4] FLOODsite. *Language of Risk: Project Definitions*. FLOODsite report T32-04-01, 2005.

[5] Folke, C. *Resilience: The emergence of a perspective for social-ecological systems analyses*, Global Environmental Change, Vol. 16 (3): 253-267, 2006.

[6] Henry, H. and Ramirez-Marquez, J. E. *Generic metrics and quantitative approaches for system resilience as a function of time.* Journal of Reliability Engineering and System Safety, Vol. 99, 114-122, 2012.

[7] UNEP. *MCA4climate: A practical framework for planning pro-development climate policies Adaptation Theme Report: Increasing Infrastructure Resilience,* 2011. Available at: http://www.mca4climate.info/_assets/files/Infrastructure-Deliverable-Final-Report.pdf [Accessed: 9 June 2017].

[8] Villagran de Leon, J.C. *Vulnerability*. *A Conceptual and Methodological Review*. Studies of the University:Research, Counsel, Education (Publication Series of UNU-EHS), 4, 2006.

[9] Zobel, C. W. *Representing perceived tradeoffs in defining disaster resilience.* Decision Support Systems, Vol. 50, 394–403, 2011.